(12) UK Patent Application (19) GB (11) 2 274 043 (13) A

(43) Date of A Publication 06.07.1994

(21) Application No 9325817.6

(22) Date of Filing 17.12.1993

(30) Priority Data
(31) 9226779 (32) 23.12.1992 (33) GB

(51) INT CL[5]
H04M 1/66

(52) UK CL (Edition M)
H4K KBHX KFD

(56) Documents Cited
US 5086459 A US 5003586 A US 4885768 A

(58) Field of Search
UK CL (Edition M) H4K KBHX KFB KFD KFF
INT CL[5] H04M 1/60 1/66 3/00 3/42
ONLINE DATABASES : WPI

(71) Applicant(s)
GPT Limited

(Incorporated in the United Kingdom)

PO Box 53, New Century Park, Telephone Road, COVENTRY, CV3 1HJ, United Kingdom

(72) Inventor(s)
Boris Vladimir Dentskevitch
Alexander Schroder Philip
Geoffrey Chopping

(74) Agent and/or Address for Service
Henry Anthony Branfield
The General Electric Company p l c,
GEC Patent Department, Waterhouse Lane,
CHELMSFORD, Essex, CM1 2QX, United Kingdom

(54) Customer identity validation to prevent fraudulent calling

(57) A security device 8 for a telecommunications system, the system having a plurality of subscriber terminals 1, 2, an exchange 7 including switching means and a connection 5 between each subscriber terminal and the exchange, the device detecting a call initiated on a connection other than from the respective subscriber terminal and including means to inhibit such a call when determined to be invalid. The detector may be connected between a subscriber terminal 1, 2 and the boundary 4 of the subscribers premises and includes means for detecting an "off-hook" condition at the detector and means for detecting signals on the connection to the exchange. The call may be inhibited by jamming. Alternatively the detector may have means for responding to a challenge message from the exchange and calculating a reply to the challenge message from a Personal Identification Number (PIN) from the subscriber terminal and returning the reply to the exchange.

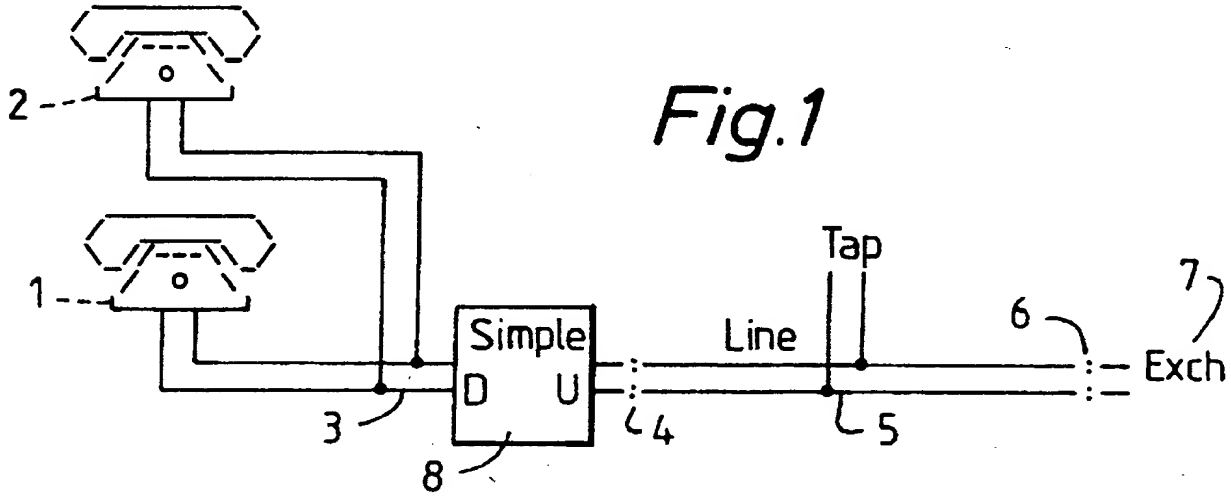


Fig.1

GB 2 274 043 A

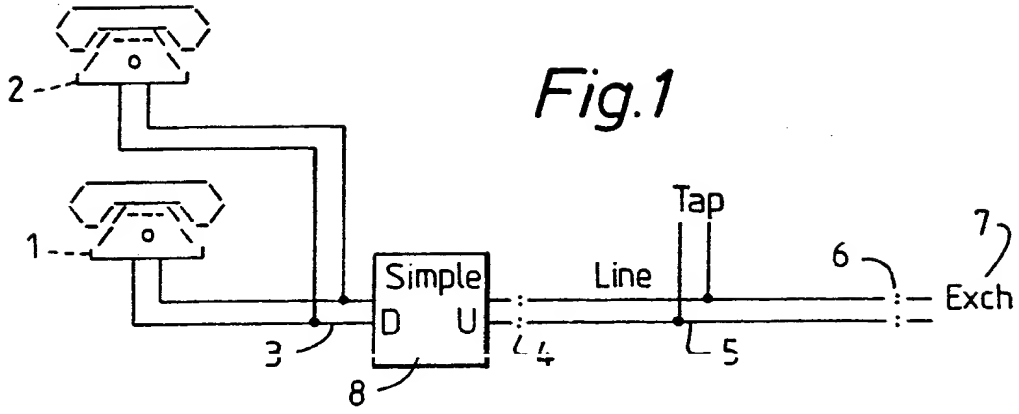


Fig.1

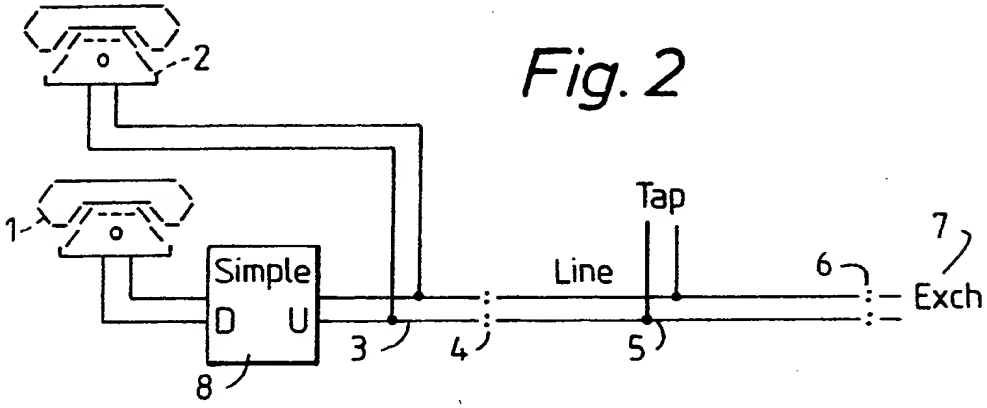


Fig. 2

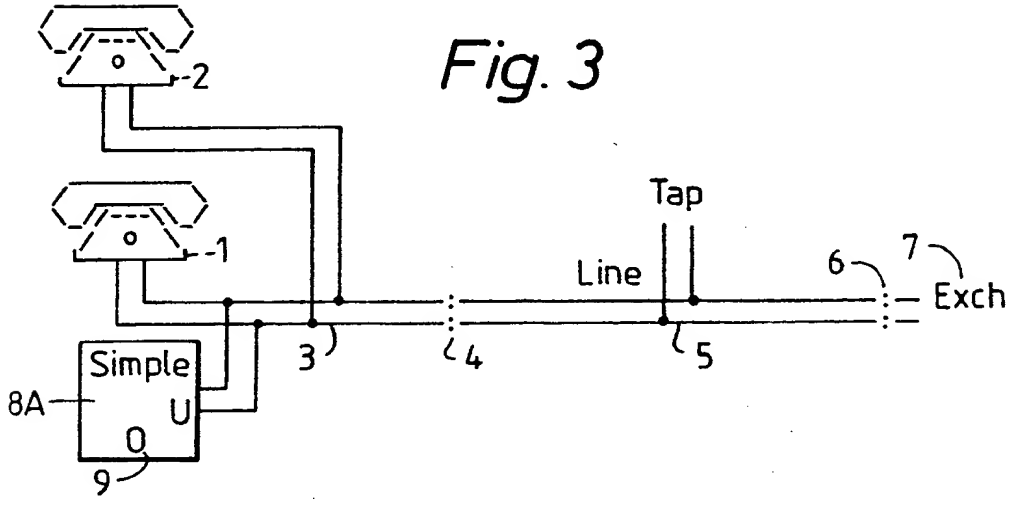


Fig. 3

Fig. 4

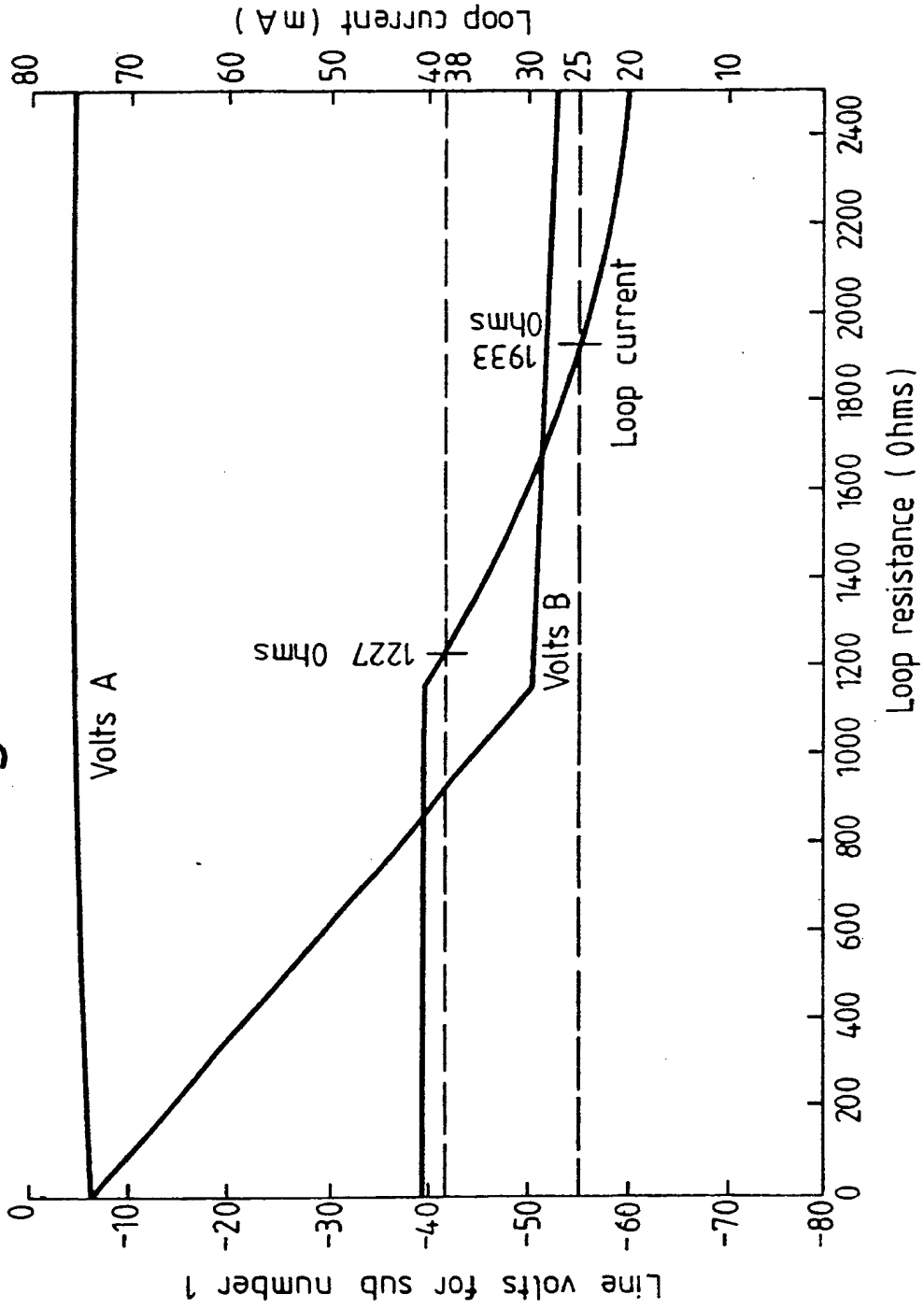

Loop current (mA)
80
70
60
50
40
38
30
25
20
10
Line volts for sub number 1
0
-10
-20
-30
-40
-50
-60
-70
-80
Loop resistance (Ohms)
0
200
400
600
800
1000
1200
1400
1600
1800
2000
2200
2400
Volts A
Volts B
1227 Ohms
1933 Ohms
Loop current

Fig.5

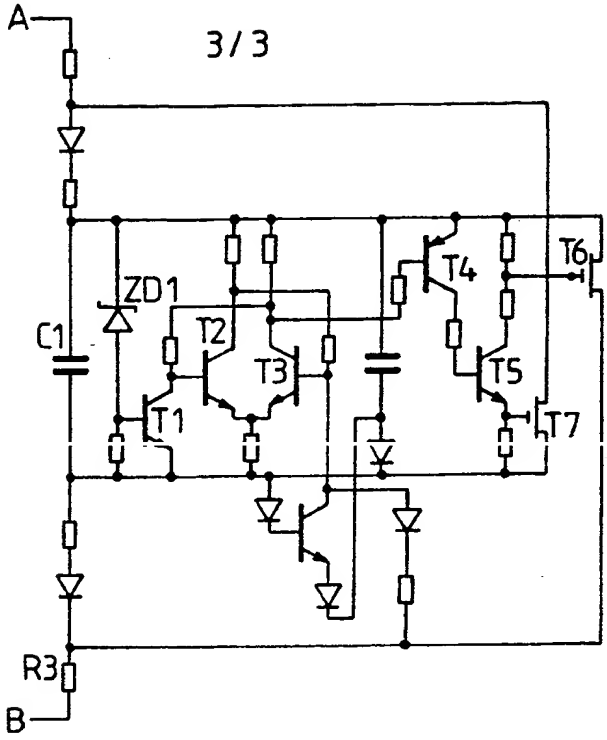
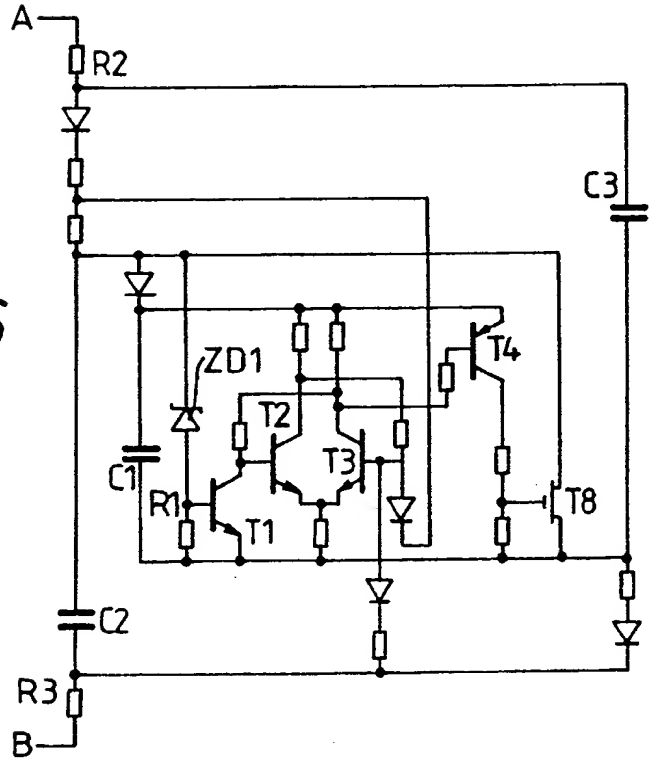

A
ZD1
C1
T2
T3
T1
T4
T6
T5
T7
R3
B

Fig.6


A
R2
C3
ZD1
T2
T4
C1
T3
R1
T1
T8
C2
R3
B

CUSTOMER IDENTITY VALIDATION

There has been increasing evidence of the making of felonious telephone calls by tapping into a customer line between the customers premises and the local exchange, such calls being charged to the customer. Areas which form prime targets for such activity are large blocks of flats where unprotected wiring goes through common areas, for example, basement car parks and utility areas and also unlocked roadside cabinets.

The telephone system operator currently has no means in most cases of determining whether a call is from such a tap or is a genuine call.

The present invention is concerned with the identification and/or prevention of unauthorised telephone calls.

According to the present invention there is provided a security device for a telecommunications system, the system comprising a plurality of subscriber terminals, an exchange including switching means and a connection between each subscriber terminal and the exchange, the device comprising a detector for detecting a call initiated on a connection other than from the respective subscriber terminal and means to inhibit such a call when determined to be invalid.

The present invention will now be described by way of example, with reference to the accompanying drawings, in which;

Figures 1-3 illustrate possible ways in which the security

unit could be connected to a telephone line,

Figure 4 shows the electrical characteristic of a line drive circuit.

Figures 5 and 6 show examples of circuits for use in the security unit.

In Figure 1 is shown a telecommunications installation having two subscriber telephones 1, 2 connected in parallel to a line 3. The line 3 passes from the subscriber's property at the boundary 4 and is in an unprotected area 5 between the boundary 4 and a further boundary 6. From the boundary 6 the line 3 passes to the exchange 7. In the unprotected area 5 a tap 8 may be connected to the line 3, providing access to the exchange 7.

Between the telephones 1, 2 and the subscribers' boundary 4, a security unit 8 may be connected. This unit 8 has a downstream interface D, to which the telephones 1, 2 are connected and an upstream interface U to which the line 3 to the exchange 7 is connected.

The unit 8 comprises means for detecting an "Off-hook" condition and also for detecting dialled and multi-frequency (MF) signals and also means for detecting whether these originated at the U or D interfaces. Any detection of these originating at the U interface will result in the call being inhibited while those originating at the D interface will not affect the call.

The inhibition of a call at its simplest can be provided by a stream of makes and breaks across the line and MF tones to prevent valid signalling reaching the exchange. Such inhibition would be considered as "jamming". The time for which it is carried on would be such as to exceed the time for which the dialling tone is available at the subscriber terminal 1, 2.

A further option available on the unit 8 would be to include within the unit means to decode any signalling detected on the D interface and to break the connection to the exchange 7 when any preprogrammed numbers are "dialled".

The unit 8 may further respond to a test line condition initiated by the exchange 7.

Where the "jamming" sequence is made to be a suitable test

sequence, the exchange 7 could connect via the test network relays (not shown) some MF tones in order to activate the "jamming" sequence.

A network operator could supply the unit 8 in order to provide better line testing through a unit 8 of their own on the subscriber's premises and also to detect abuse of the telephone line on which they would incur the cost of repairs.

The unit 8 could include provision for an indication, either visual or audible, that the "jamming" sequence has been activated.

In Figure 2 an alternative arrangement is shown, the same reference numerals being used as in Figure 1. The only difference is that the telephone 2 is connected on the upstream side of the unit 8. As a result outgoing calls can be made from telephone 1, but not from telephone 2, without activating "jamming".

In Figure 3 is shown a further alternative arrangement in which the unit 8A is only connected to the line 3 at the U interface. The D interface is either not connected or may not exist. The unit 8A would include an inhibit button 9.

As use of either of the telephones 1, 2 would activate the "jamming" sequence, operation would need the button 9 to be pressed which would allow a period during which calls would be permitted.

The unit 8A could be less complicated as it does not need to differentiate between "Off-hook" dialled pulses and MF signals on the U and D interfaces.

The description so far has referred to telephones as the subscriber terminal, but it does not need to be restricted to a telephone. Other types of subscriber terminals, such as for example, fax machines, modems and computers are also considered as being encompassed by the present invention.

There follows a description of various variations in the present invention. The specific examples are directed to operation using facilities provided on the British Telecom (BT) network, but similar facilties are provided by other network operators, differing only in the codes used.

At its simplest the 'off-hook' condition can be detected by the line current, using two back-to-back diodes in one leg of the subscriber line at the first entry point to the subscriber premises.

Any terminal going off-hook in the premises will generate about ¾ volt, while any connection external to the premises will not. To provide protection in unattended premises a key-operated switch could be used to short-circuit the device.

The line-current signal could be used to send a DTMF PIN-code which the local exchange concentrator would check before applying dial tone.

Security breaches have occurred by stealing telephone terminals used on the Mercury network, these terminals having the account number in the memory, and using the terminals elsewhere. The PIN-code from the device could have the equipment number encoded into it so that the terminal would be useless on another exchange line.

On the BT network what are known as "Level 1" codes provide access to various services. These are codes the first digit of which is 1.

Examples are:-

100 - calls via operator
153 - International Directory Enquiries
155 - Calls via International operator
193 - National Directory Enquiries
151 - Fault repairs
17* - Used for maintenance purposes.

Of these the first four are numbers which result in charges to the subscriber and the last two do not result in charges, though it is unlikely that a person tapping into the line would want to make use of the 151 code.

When maintenance is being carried out, frequently it is done without access to the subscribers premises.

The engineer carries out any testing by connecting to the wires on a pole or in a street cabinet or manhole. Unfortunately, to

the security unit this appears as tapping and the engineer will be unable to carry out testing.

In such a circumstance a procedure such as detailed below could be instituted.

SIMPLE SEQUENCE

1 Initial state.

2 In the absence of a downstream loop, if the security unit detects MF signalling at any time, it will initiate Jamming (20).

3 In state 1, if the security unit detects an upstream LOOP it will apply its own loop (4).

4 Application of own loop (prevents loop disconnect signalling). Start 3 second wait.

5 If during 3 second wait Dial Tone is detected, to go 9.

6 If During 3 second wait dial tone is not detected, remove own loop and go to initial state 1.

7 In state 1, in the absence of a downstream loop, if a detects Dial Tone is detected, it will apply its own loop (8).

8 Application of own loop (prevents loop disconnect signalling). Start 3 second wait.

9 If Dial Tone does not persist to end of 3 second wait, initiate Jamming (20).

10 Remove own loop for 50 ms, if upstream loop is present during 50 ms, initiate Jamming (20).

11 Start 2 second wait.

12 If during wait dial tone is removed go to 14.

SIMPLE SEQUENCE

13 If 2 second wait finishes (dial tone still present), initiate jamming (20).

14 Remove own loop SEVEN times (50 ms off 50 ms on), if upstream loop is present during any 50 ms removals,

initiate Jamming (20).

15 Start 15 seconds wait.

16 If upstream loop applied, start 300 second wait.

17 During 300 second wait, if upstream loop is removed for one second, go to initial state (1).

18 At end of 300 seconds, initiate Jamming (20).

19 At end of 15 second wait, go to initial state (1).

20 Jamming. Maintain LOOP and JAM audio frequencies for 60+ * seconds after which remove loop and JAMMING.

21 Set Activation Light. Go to initial state (1).

(* Long enough for exchange to time-out.)

TEST ENGINEER SEQUENCE

Attach test instrument.
Go off hook for 1 to 2 seconds and immediately go on hook.
Wait 10 seconds.
Go off hook again.
Listen for dial tone.
If dial tone is heard then there is no simple connected and normal test dialling sequence should be used.
If no dial tone is heard then there may be a security unit connected which has dialled - ONE - SEVEN.
Start dialling from after the - ONE - SEVEN.
If code does not work, a security unit may not exist and the exchange may not be supplying dial tone.
Go off hook to check for lack of dial tone.
If jamming is heard wait 2 minutes and try again.

TEST ENGINEER USING MF

Sending the MF code - ONE will cause the security unit to JAM for 60* seconds. Therefore remove loop wait for more than 60* seconds and proceed with loop disconnect procedure.

The detection of a tap or the subscribers use of a line could be carried out by the detection of a change in the line voltage. While this is generally effective, there are problems when a high resistance tap is placed on a short line or on a long line near the exchange.

This can be seen from Figure 4 which shows the characteristics of the line drive circuits. If the loop impedance is of the order of 2000 ohms, then there will be no change in voltage on the line.

If a similar impedance is applied at the end of a long line then there will be a voltage change at the security unit because the line and the tap act as a voltage divider.

An alternative way of detecting a tap is to provide a line reversal on answer, so that the normal arrangement of line polarity (line A at OV and line B at -50V) is a reversed for the length of the call.

This would be very easy to detect providing that this line reversal was distinguished from the line reversal that occurs during ringing. While this option is available on modern exchanges, most lines are not set to operate in this manner.

Line reversal is a feature of payphones and payphones containing all the charging intelligence.

Any tapping of a payphone line is a direct loss to the system operator. A security unit could be connected within a payphone and hence would be inherently protected.

Considering the construction of a security unit as referred to above, in order to make a call on an ordinary telephone line, the line has first to be seized by applying a low resistance across the pair of wires. The resultant current flow is detected in the exchange and if it is large enough and persists for long enough the exchange starts the call procedure by sending out dial tone.

It is important that the security unit can detect a fraudulent seize, wherever the tap is applied along the length of the line. Some telephone lines are very long and can have a loop resistance of 1800 ohms. So a tap applied at the exchange end of the line is harder to detect at the subscriber end, especially if quite a

high value of resistance is used to seize the line.

Modern line circuits have a constant voltage characteristic which unfortunately often prevents a tap, applied at the exchange end, from being observed at the subscribers end using just passive monitoring.

Not only must a seize be detected but also any subsequent signalling.

The signalling applied to the line can be Multi-Frequency (MF) or Loop Disconnect.

Once the line has been seized and MF signalling has started, the only way of preventing the illegal call attempt is for the security unit to jam the line to prevent the completion of the MF signalling phase and any conversation. Jamming will normally continue until the seize is removed.

However, once the line has been seized, if loop disconnect signalling starts, then any further signalling can be prevented by the security unit applying a seize, as this will stop the exchange recognising any further loop disconnect signalling.

Because a maintenance engineer may require to tap a line to call the exchange, it must be possible for this to still be done. The numbers dialled should only be in the 17x range. No chargeable calls should be made by maintenance engineers tapping a line. In order to stop fraudulent calls from people acting like maintenance engineers, or dishonest maintenance engineers, tapped calls must be restricted to 17x, or any other agreed non-chargeable range.

Of course a genuine maintenance engineer will use a normal value of seize resistance. The effect of a normal seize resistance being briefly removed for every looped dialling pulse is easily monitored by the security unit.

Provided that the detected loop disconnect signalling consists of a ONE followed by a SEVEN and one other digit, then the security unit will not apply to its own parallel seize until 10 seconds after it detected the original seize, so that the maintenance call can proceed. Maintenance calls are not charged to the subscriber.

A further sequence will also be accepted which will

initiate the test sequence described later.

Following a detected seize, if no MF signalling, or no loop disconnect signalling, or any other recognised loop disconnect sequence is detected by the security unit, then a parallel seize will be applied after 10 seconds as will MF jamming. As MF jamming is very audible any attempt at making chargeable calls via the switchboard operator will be prevented.

After a time-out period the security unit will release its parallel seize and MF jamming. It will then start monitoring to see if the original seize is still present. If the seize is still present then the parallel seize will be reapplied.

Monitoring changes in the line voltage will normally be apparent, when a normal maintenance handset is attached near the subscribers premises. Consequently a basic monitoring method may be considered sufficient for some circumstances. However the following arrangements, outlined below, both provide comprehensive methods of detecting a seize.

The security unit of course can differentiate between seizes on the exchange side and on its own subscriber side by noting any voltage drop in a low value series resistance which is permanently inserted.

Even applying a short duration seize (mini-seize), at the end of a long line, may not bring the exchange line circuit out of its constant voltage mode.

However by applying a reverse voltage at the end of the line, as part of a mini-seize, enough current will be drawn for a short period of time in order to detect the presence of a tap.

In order to detect a seize the following procedure is carried out as shown in Figure 5. A capacitor C1 is trickle charged from the line feed current until it is charged to a large percentage of the line voltage. The capacitor is then partially discharged, with reverse polarity, into the line in series with a seizing resistance. This process of charging followed by discharging is continually repeated and only draws a low mean current.

Even if a tap does not significantly affect the charging time of the capacitor, it will affect the discharging time of the

capacitor.

In Figure 5, a capacitor C1 is connected across the line terminals A, B and charges up from the line current. A zener diode ZD1 with a series resistor R1 is connected in parallel with the capacitor C1. When the voltage across the capacitor C1 exceeds the zener voltage, the zener diode ZD1 is biassed into conduction and transistor T1 is switched 'on', which results in the transistors T2, T3 of the cross-linked long-tailed pair being turned 'off' and 'on' respectively. Consequently, the FET's T6, T7 are turned 'on'via the transistors T4, T5 and as a result the capacitor C1 is re-connected with its polarity reversed between the line terminals A, B and discharges into the line through series seizing resistors R2, R3. The purpose of the remaining components is to reset the transistors T2, T3 and to prevent circuit 'lock-up' at initiation of the supply.

If the security unit significantly increases the line voltage at the subscribers end, by injecting a voltage source onto the line, this will cause some of the current drawn by an illegal tap to be supplied by the security unit, and the presence of a high resistance seize at the exchange end of the line can be determined.

As shown in Figure 6, in order to detect a seize the following procedure is carried out. Two capacitors C2, C3 are trickle charged from the line feed current until they are both charged to a large percentage of the line voltage. The capacitors are joined in series across the line and partially discharged back into the line. This process of charging followed by discharging is continually repeated and only draws a low mean current.

A tap may not significantly affect the charging time of the capacitors, but it will affect the discharging time of the capacitors.

In Figure 6, the majority of the circuit functions in a similar manner to the circuit of Figure 5, as is indicated by similar references. There are two further capacitors C2, C3 which are charged to the line voltage. When the transistor T4 is turned 'on', the FET T8 is turned on and the capacitors C2, C3 are connected in series across the line terminals providing a higher than normal voltage therebetween. Various additional features can be provided

simply.

Although the polarity of a subscribers line is defined the unit will indicate if the polarity is inverse and a switch can be changed so that it will function from reversed polarity.

The security unit can also be arranged to provide an audible or visual indication if the line loses power for longer than the normal line testing period. This means that the subscriber can ask for the line to be repaired, as soon as they hear the audible warning tone or see the flashing indicator, rather than waiting until they next try and use the phone.

If the telephone line is deliberately disconnected or cut in order to make an illegal call, the unit will indicate that the line had lost power for some time.

The exchange could activate the unit by applying a seize for a short period followed by a special loop disconnect signalling sequence and waiting for the unit to apply a short burst of MF jamming without reporting an attempt at making an illegal call.

The exchange will then be very confident that there is a good path all the way to the subscribers premises, if it receives back the single burst of MF jamming at the expected amplitude level.

If the reply is two bursts of MF jamming then it will mean that the unit has taken protective action against an illegal call attempt in the last 24 hours.

If the reply is three bursts of MF jamming then it will mean that there has been a significant line power interruption in the last 24 hours.

When a fraudulent call can be made from one telephone line and charged to second line, having a security unit attached to the second line will not prevent this type of fraud.

As the BT network does not forward the calling line identity to the Mercury network, Mercury currently charge the owner of the Personal Identification Number (PIN) supplied at the start of a call.

Because there are several ways of discovering a Mercury PIN, it will be very useful for the Mercury exchange to be able to verify that the person making the call is doing so from the

customer's premises.

An alternative unit can be attached to a subscriber's line at the subscriber's premises.

Once the subscriber has initiated the call through to the Mercury exchange, the Mercury exchange will issue the subscriber with a Challenge to verify that the call is coming from the correct premises.

The Challenge message is sent out using the same modem unit that is used for the CLASS (Custom Local Area Signalling System) messages.

The Challenge message is received by a CLASS detection circuit in the unit. The Challenge message includes a large binary number that is especially generated for that call.

The unit hardware contains its own large PIN that is programmed in during manufacture and which cannot be changed.

The unit performs a mathematical function such as a form of division. For example it divides the Challenge number by its own PIN. Challenges are chosen so that remainders result. A way of achieving this is by only using primary numbers for challenges and PINs.

Using octal coding and a sequence of 4 MF signalling tones, the unit supplies 12 binary bits selected from the remainder.

By checking the 12 returned binary bits with its own calculation the Mercury exchange can then verify that the correct unit is at the calling subscriber's premises.

Because the PIN is not transmitted, the monitoring of the line will not reveal the PIN. Neither can the PIN be deduced from the Challenge and the remainder, unless a very large number of calls are monitored.

The principle of a challenge could also be employed with charge cards, where they are used with a card reader. Part of the information contained on a charge card could be signalled directly to the exchange and part could be used, by the card reader unit, along with a challenge message, received from the exchange, to create a remainder. The full details of a charge card and a subscribers PIN could not then be determined by just monitoring the line.

Units connected at customer premises are very often owned by the customer.

Therefore it is sensible not only to consider supplying CLASS, and the two types of security unit as separated units, but also as combined units. In some cases, combining them with the telephone instrument itself may be appropriate.

Because of the acceptance by the network operators that they are liable for the cost of fraudulent calls, it is possible that they may wish to install one or other or both units sealed in the master socket. This will not only greatly help to prevent fraud by third parties but also fraud by the subscribers when they make calls and then claim that they had not made them. The test responses of the first unit should also be attractive to the network operators as it should make the identification of some faults easier and therefore help to indicate whether it is a fault within the subscriber's equipment or the network operator's equipment.

CLAIMS

1. A security device for a telecommunications system, the system comprising a plurality of subscriber terminals, an exchange including switching means and a connection between each subscriber terminal and the exchange, the device comprising a detector for detecting a call initiated on a connection other than from the respective subscriber terminal and means to inhibit such a call when determined to be invalid.

2. A security device as claimed in Claim 1, wherein the detector is connected to the connection between a subscriber terminal and the boundary of the subscribers premises and comprises means for detecting an "off-hook" condition at the detector and means for detecting signals on the connection to the exchange.

3. A security device as claimed in Claim 1 or 2 wherein the call is inhibited by jamming.

4. A security device as claimed in Claim 3 wherein the jamming is provided by a stream of "makes" and "breaks" across the line or a series of multi-frequency (MF) tones.

5. A security device as claimed in Claim 2 or any claim appendent thereto further comprising means to decode any signal detected and to inhibit a call when preprogrammed numbers are detected.

6. A security device as claimed in any preceding claim further comprising means to respond to a test signal from the exchange.

7. A security device as claimed in Claim 1, wherein the detector comprises means for responding to a challenge message from the exchange and calculating a reply to the challenge message from a Personal Identificaton Number (PIN) from the subscriber terminal and returning the reply to the exchange.

8. A security device as claimed in Claim 7, wherein the PIN is held within the subscriber terminal.

9. A security device as claimed in Claim 7, wherein the PIN is provided on a card read by a card reader forming part of or attached to the subscriber terminal.

10. A security device substantially as hereinbefore described, with reference to and as illustrated in the accompanying drawings.

Patents Act 1977
Examiner's report to the Comptroller under Section 17
(The Search report)

Application number
GB 9325817.6

Relevant Technical Fields

(i) UK Cl (Ed.M) H4K (KBHX,KFB,KFD,KFF)

(ii) Int Cl (Ed.5) H04M (1/00,1/66,3/00,3/42)

Search Examiner
Mr S J L Rees

Date of completion of Search
29 March 1994

Databases (see below)
(i) UK Patent Office collections of GB, EP, WO and US patent specifications.

(ii) ONLINE DATABASES : WPI

Documents considered relevant following a search in respect of Claims :-
1-10

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family; corresponding document.

Category	Identity of document and relevant passages		Relevant to claim(s)
X	US 5086459	(KEPTEL) whole document especially column 6 lines 8-29	1,2
X	US 5003586	(SIECOR) whole document especially column 3 line 57 to column 4 line 45	1,2
X	US 4885768	(GENIN) whole document especially column 4 lines 32-63	1,2,5, 6,7

Databases:The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).